НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___”_____20 _ р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки : 113 «Прикладна математика»
(код і назва)

на тему: Оцінювання стійкості незбалансованої схеми MISTY до диференціальних та лінійних криптоатак.

Виконав: студент 4 курсу, групи ФІ-62
(шифр групи)

Кашуба Артем Костянтинович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник Яковлєв Сергій Володимирович, к. т. н., доцент _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут

Кафедра математичних методів захисту інформації

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки - 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою

М.М.Савчук

_____
(підпис) (ініціали, прізвище)

«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту

Кашуба Артем Костянтинович
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінювання стійкості незбалансованої схеми MISTY до диференціальних та лінійних криптоатак,
керівник роботи Яковлєв Сергій Володимирович, к. т. н., доцент ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____ р. № _____

2. Термін подання студентом роботи _____

3. Вихідні дані до роботи _____
_____
_____
_____

4. Зміст роботи дослідження властивостей лінійних потенціалів та диференціальних імовірностей для незбалансованої однорідної MISTY-подібної схеми; дослідження впливу лінійної частини раундової функції незбалансованої однорідної MISTY-подібної схеми на її стійкість до диференціального та лінійного криптоаналізу.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____

_____

_____

_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Узгодження теми дипломної роботи з керівником	01.09. – 01.10.	
2	Пошук та опрацювання інформації сумісної до теми диплому	01.10. – 01.12.	
3	Дослідження властивостей диференціальних ймовірностей для незбалансованої однорідної MISTY-подібної схеми	01.12. – 01.01.	
4	Дослідження властивостей лінійних потенціалів для незбалансованої однорідної MISTY-подібної схеми	01.01. – 10.03.	
5	Дослідження впливу лінійної частини раундової функції незбалансованої однорідної MISTY-подібної схеми за показниками стійкості	10.03. – 15.05.	
6	Оформлення роботи	15.05. – 04.06.	

Студент _____ Кашуба А.К.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Яковлєв С.В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Кваліфікаційна робота містить: 47 стор., 18 рисунків, 0 таблиць, 10 джерел.

Метою даної роботи є поширення та узагальнення формальної теорії диференціального та лінійного криптоаналізу на класи незбалансованих Фейстель-подібних схем. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження є криптографічні властивості незбалансованих Фейстель-подібних схем.

В цій роботі було розглянуто варіант незбалансованої схеми MISTY невеликого розміру, для якого експериментально були обчислені значення диференціальних імовірностей та лінійних потенціалів, які характеризують стійкість таких схем, в залежності від використаних S-блока та лінійного перетворення.

Експериментально було отримано вісім функцій L, які дають гарантовану стійкість до диференціального криптоаналізу, тобто для будь-якого S-блока при таких функціях показник MDP шифру буде мати нетривіальну фіксовану верхню межу.

Первинний аналіз отриманих найкращих лінійних перетворень показав, що для таких функцій не присутні явні особливості, що підсилюють стійкість досліджуваної схеми до диференціального криптоаналізу.

Також було показано, що функції L, які є найкращими з точки зору стійкості до диференціального криптоаналізу, не являються найкращими та найгіршими у випадку з лінійним криптоаналізом, оскільки їх поведінку не можна назвати стабільною.

БЛОКОВІ ШИФРИ, СИМЕТРИЧНА КРИПТОГРАФІЯ, ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ, ЛІНІЙНИЙ КРИПТОАНАЛІЗ, НЕЗБАЛАНСОВАНА СХЕМА MISTY

ABSTRACT

The qualifying paper contains: 47 pages, 18 figures, 0 tables, 10 sources.

The purpose of this paper is to to extend and generalize the formal theory of differential and linear cryptanalysis to classes of unbalanced Feistel-like schemes. The object of research is information processes in cryptographic protection systems. The subject of the research is the the cryptographic properties of unbalanced Feistel-like schemes.

In this paper, we considered a variant of the unbalanced MISTY network of small size, for which were experimentally calculated the values of differential probabilities and linear potentials that characterize the stability of such networks, depending on the used S-block and linear transformation.

Experimentally were obtained 8 L functions which provide guaranteed resistance to attacks from the side of differential cryptanalysis, in other words, for any S-block with such functions, the cipher MDP index will have a fixed non-trivial upper limit.

The initial analysis of the obtained best linear transformations showed that for such functions there are no obvious features that enhance the stability of the studied scheme to differential cryptanalysis.

It has also been shown that the L functions which are the best in terms of resistance to differential cryptanalysis are not the best and worst in case of linear cryptanalysis, because their behavior cannot be called stable.

BLOCK CIPHERS, SYMMETRICAL CRYPTOGRAPHY, DIFFERENTIAL CRYPTOANALYSIS, LINEAR CRYPTOANALYSIS, UNBALANCED MISTY NETWORK

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$\oplus$ — операція побітового додавання

V_n — простір двійкових векторів дожини n

$\overline{\sum_x}$ — усереднена сума за всіми значеннями x

$[P]$ — індикаторна функція

$MDP_{\oplus}^{f_k}$ — максимальна диференціальна імовірність функції f

$MELP^{f_k}$ — усереднений лінійний потенціал функції f_k

$\Phi[f_1, \ldots, f_r]$ — схема Фейстеля із раундовими функціями $f_i, i = \overline{1, r}$

ВСТУП

Актуальність дослідження. В умовах сьогодення існує досить велика кількість симетричних блокових шифрів, метою проектування яких є створення надійного алгоритму, який виконується за розумний час на доступному обладнанні, та достатньо простий в реалізації.

Існує безліч атак, яким блокові шифри змушені протистояти. Серед таких атак виділяють лінійний та диференціальний криптоаналіз. Блокові шифри відрізняються між собою складністю реалізації та різними показниками стійкості з точки зору атак диференціального та лінійного криптоаналізу.

Для великої кількості існуючих блокових шифрів було отримано теоритичні оцінки стійкості до диференціальних та лінійних криптоатак, однак деякі перспективні схеми досі не були досліджені належним чином: для них теоритичних оцінок немає.

Метою дослідження є поширення та узагальнення формальної теорії диференціального та лінійного криптоаналізу на класи незбалансованих Фейстель-подібних схем. Для досягнення мети необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) дослідити властивості диференціалів незбалансованої однорідної MISTY-подібної схеми;

3) дослідити властивості лінійних потенціалів незбалансованої однорідної MISTY-подібної схеми;

4) дослідити вплив лінійної частини раундової функції незбалансованої однорідної MISTY-подібної схеми на її стійкість до диференціального та лінійного криптоаналізу.

Об'єкт дослідження: інформаційні процеси в системах криптографічного захисту.

Предмет дослідження: криптографічні властивості незбалансованих

Фейстель-подібних схем.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної та абстрактної алгебри, теорії імовірностей, методи комп'ютерного та статистичного моделювання.

Наукова новизна. Вперше експериментально показано, що криптографічні властивості незбалансованих Фейстель-подібних схем суттєво залежать від лінійної функції, яка змішує праву та ліву частину вхідного блоку. Показано, що для малих шифрів можна обрати такі лінійні функції, які будуть давати гарантовану стійкість до диференціального криптоаналізу.

Практичне значення. Результати даної роботи можна використати для побудови нових криптографічно стійких блокових шифрів, або їх складових елементів.

Апробація результатів та публікації. Частина результатів даної роботи було представлено на Всеукраїнській науково-практичній конференції «Теоретичні та прикладні проблеми фізики, математики та інформатики» (12-13 травня 2020 року, м.Київ).

1 ФЕЙСТЕЛЬ-ПОДІБНІ СХЕМИ ТА ІСНУЮЧІ ТЕОРЕТИЧНІ ОЦІНКИ ЇХ СТІЙКОСТІ

У даному розділі розглядається поняття ітеративного блокового шифру, основні види Фейстель-подібних схем, основні положення диференціального та лінійного криптоаналізу. Також розглянуто деякі існуючі теоретичні оцінки стійкості Фейстель-подібних схем з точки зору атак диференціального та лінійного криптоаналізу.

1.1 Ітеративні блокові шифри та Фейстель-подібні схеми

Нехай M — множина відкритих текстів, Y — множина шифртекстів, K — множина ключів, V_n — множина всіх бітових векторів довжини n. *Шифруючим перетворенням* називається функція вигляду

$$f : M \times K \to Y,$$

що задовольняє таким умовам: для кожного фіксованого значення $k \in K$ перетворення $y = f_k(x)$ є бієктивним.

Ітеративний r-раундовий блоковий шифр E — перетворення виду $E : V_n \times K^r \to V_n$, що є композицією r шифруючих перетворень:

$$E = F_{k_1}^{(1)} \circ F_{k_2}^{(2)} \circ ... \circ F_{k_r}^{(r)}.$$

Функції $F_{k_i}^{(i)}$ будемо називати *раундовими перетвореннями*, а змінні k_i — *раундовими ключами*. Тут і надалі будемо вважати, що раундові ключі (k_1,k_2,...,k_r) є випадковими, незалежними та рівномірно розподіленими в ключовому просторі.

Схема Фейстеля — це ітеративний блоковий шифр, у якому кожне раундове перетворення задається таким співвідношенням:

$$F_k(x, y) = (y\ ,\ x \oplus f_k(y)).$$

Тут ми вважаємо, що вхідний блок розбивається на дві рівні частини x та y, k — раундовий ключ.

Даний шифр був створений Хорстом Фейстелем при проектуванні шифру Lucifer і з тих пір використовувався в багатьох конструкціях блокових шифрів - таких, як: DES, FEAL, GOST, LOKI, CAST, Blowfish та RC5.

Кожне раундове перетворення такої схеми має вигляд, зображений на рис. 1.1.

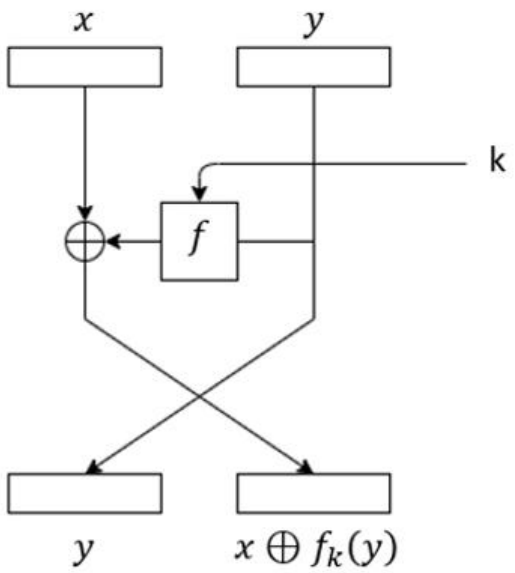

Рисунок 1.1 – Один раунд схеми Фейстеля

Фундаментальним будівельним блоком схеми Фейстеля є f-функція, що визначається таким чином:

$$f : \{0,1\}^{n/2} \times \{0,1\}^{k} \to \{0,1\}^{n/2}\ ,$$

де n — довжина вхідного блоку, f — це функція, що приймає на вхід $n/2$ бітів вхідного блока (на рисунку 1.1 це y) та k бітів раундового ключа, а

результатом цієї функції є бітовий вектор дожини $n/2$. Слід зазначити, що f може бути як S-блоком (блоком підстановок), P-блоком (блоком перестановок), циклічним зсувом, додаванням або множенням за певним модулем.

Схема блокового шифрування називається схемою Фейстеля, якщо вона записується таким чином:

$$E_k(x,y) = swap(F_{k_r}(...F_{k_1}(x,y)...)),$$

де r — кількість раундів шифрування, $swap(x,y) = (y,x)$. В подальшому будемо позначати r-раундову схему Фейстеля як $\Phi[f_1, \ldots, f_r]$.

Схема MISTY [1] (Mitsubishi Improved Security Technology) - це ітеративний блоковий шифр, створений у 1996 році криптологом Міцуру Мацуї на основі схеми Фейстеля; також її називають L-схемою. Один раунд класичної схеми MISTY записується таким чином:

$$F_k(x, y) = (y, y \oplus f_k(x)).$$

Структуру раундового перетворення зображено на рис. 1.2.

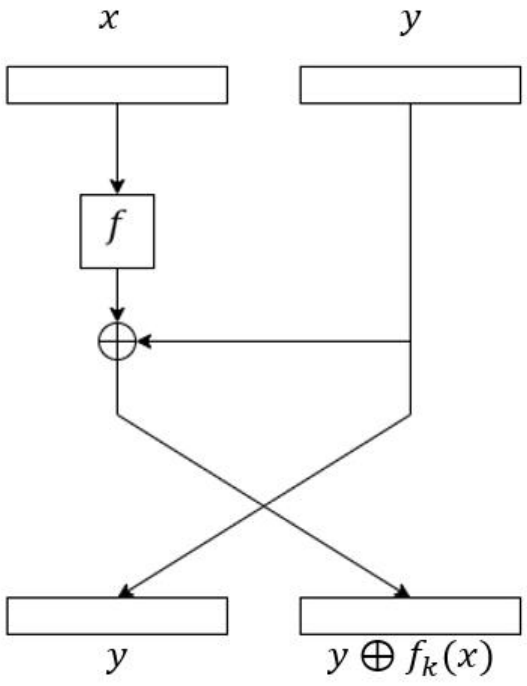

Рисунок 1.2 – Один раунд схеми MISTY

R-схемою називають ітеративний блоковий шифр, один рауд якого задається таким співвідношенням:

$$F_k(x, y) = (y \oplus f_k(x), f_k(x)).$$

Узагальнені схеми Фейстеля [2] — це схеми Фейстеля, у яких вхідний блок розбивається на два та більше підблоки, частина з яких на кожному раунді перетворюється за деяким законом. Якщо довжини підблоків співпадають — такі схеми називають збалансованими, в протилежному випадку — незбалансованими.

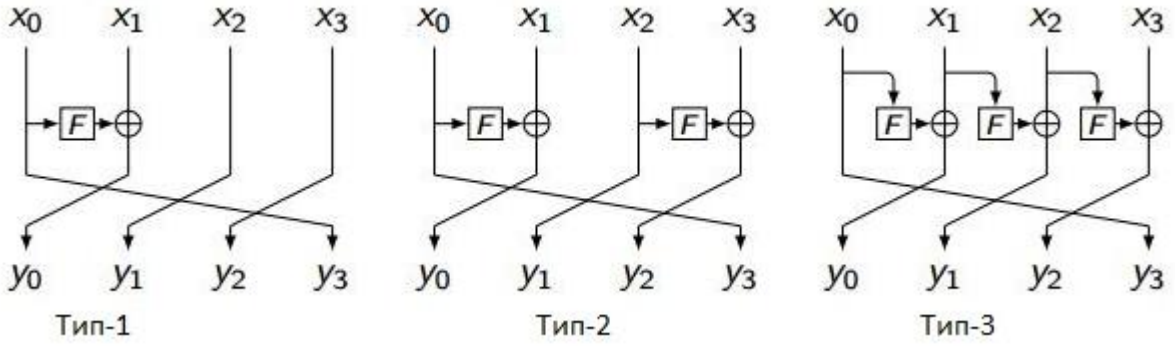

Рисунок 1.3 – Деякі узагальнені схеми Фейстеля

На рис. 1.3 зображені типи узагальнених схем Фейстеля, які найчастіше використовуються.

Основною перевагою таких схем являється більш легке опрацювання збільшених блоків тексту (бітових рядків) для їх подальшого шифрування.

Незабалансована схема Фейстеля [3] — це схема Фейстеля, у якій правий та лівий вхідні підблоки мають різну довжину. Структура раундового перетворення має вигляд, зображений на рис. 1.4.

Нехай s - довжина блока x, t - довжина блока y, n - довжина вхідного блока, тоді один раунд незбалансованої схеми Фейстеля задається таким співвідношенням:

$$F_k(x, y) = (f_k(x) \oplus y, x),$$

де k – раундовий ключ, $f_k : V_s \to V_t$.

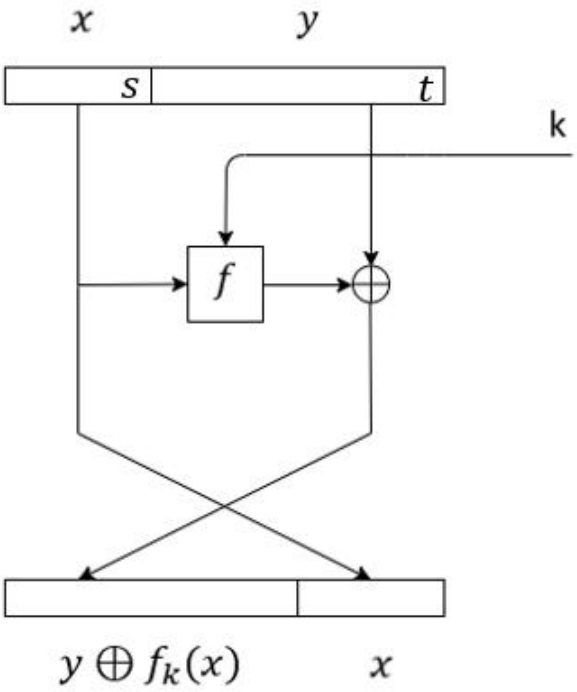

Рисунок 1.4 – 1 раунд незбалансованої схеми Фейстеля

Блок x називається *джерельним блоком (source block)*, а блок y - *цільовим блоком (target block)*. Відповідно, незабалансовані схеми Фейстеля, для яких $s > t$ називаються *джерельно важкими (source heavy)*, та *важкоцільовими (target heavy)*, якщо $s < t$.

Незбалансована схема Фейстеля є *однорідною (homogenous)* [3], якщо функція f_k ідентична на кожному раунді, окрім раундових ключів, і вона є *неоднорідною (heterogenous)* [3], якщо для різних раундід функція f_k не завжди однакова.

Основна перевага неоднорідних незбалансованих схем Фейстеля полягає в більш складному виявленні будь-яких характеристик, що можуть стати у нагоді криптоаналітику, оскільки внутрішні властивості таких схем змінюються від раунда до раунда. Однак реалізувати таку мережу часто набагато складніше за однорідну.

Також можливий варіант, коли не всі біти вхідного блоку використовуються в кожному раунді незбалансованої схеми Фейстеля.

Незбалансована схема Фейстеля називається *повною* [3], якщо $s + t = n$, тобто коли кожен біт віходного блоку є частиною або цільового, або джерельного блоку. Незбалансована схема Фейстеля називається *неповною*, якщо $s + t < n$. В неповних схемах, де $n - s - t = z$ бітів не є частиною цільового чи джерельного блока, називається нульовим блоком (null block).

Незаблансована схема Фейстеля називається *послідовною (consistent)* [3], коли s, t, n, z залишаються незмінними протягом усіх раундів шифрування. В іншому випадку такі схеми називають *непослідовними (inconsistent)*.

Цикл [3] — це кількість раундів, необхідних для кожного з бітів в блоці для проходження через джерельний блок і цільовий блок як мінімум один раз.

Коефіцієнтом премішування (rate of confusion) [3] послідовної незбалансованої схеми Фейстеля є мінімальною кількістю раундів, що необхідно для проходження кожного з бітів через цільовий блок. Ця величина позначається як R_c, для неї справедливе наступне твердження:

$$R_c \leq \frac{t}{n}.$$

Нехай X_i — вхідний блок на i-му раунді незбалансованої схеми Фейстеля. Будь яка зміна в блоці X_i повинна мати деякий шанс змінити кожен біт в X_{i+m} для деякого m. Процес, при якому один біт в блоці може вплинути на інші біти в деякому наступному блоці називається розсіюванням.

В незбалансованих схемах Фейстеля деякий біт j вхідного блоку може вплинути на інші біти в блоці тільки якщо біт j належить джерельному блоку. *Коефіцієнтом розсіювання (rate of diffusion)* [3] послідовної незбалансованої схеми Фейстеля називається мінімальна кількість разів за цикл, при якій даний біт має можливість впливати на інші біти в блоці. Ця величина позначається як R_c, для неї справедливе наступне твердження:

$$R_d \leq \frac{s}{n}$$

1.2 Диференціальний криптоаналіз

Диференціальний криптоаналіз відноситься до так званих атак останнього раунду, оскільки основною метою проведення аналізу є встановлення раундового ключа останнього раунду.

Цей метод працює з парами шифрованих текстів, відкриті тексти яких мають деяку різницю. Криптоаналітик аналізує еволюцію цієї різниці в процесі проходження відкритих текстів через етапи шифрування одним і тим же ключем.

Нехай $f : V_n \to V_n$ - булева функція. Тоді $\oplus$ - диференціалом називається деяка пара векторів (α,β), для якої існує подія $\alpha \xrightarrow{f} \beta$, що для випадкового значенная x входу функції виконується наступна рівність:

$$f(x \oplus \alpha) = f(x) \oplus \beta.$$

Імовірністю диференціала називається усереднена за усіма можливими значеннями x сума

$$DP^f_{\oplus}(\alpha,\beta) = \frac{1}{2^n} \sum_{x \in V_n} [f(x \oplus \alpha) = f(x) \oplus \beta],$$

де квадратні дужки позначають індикаторну функцію.

Максимумом диференціальної імовірності функції f називається величина

$$MDP_{\oplus}(f) = \max_{\alpha,\beta \neq 0} DP^f_{\oplus}(\alpha, \beta).$$

Для шифруючого перетворення f_k справедливим є означення імовірності диференціалу:

$$DP^{f_k}_{\oplus}(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in V_n} [f_k(x \oplus \alpha) = f_k(x) \oplus \beta].$$

Щоб провести атаку, слід знайти імовірності диференціалів та обрати диференціали з високою імовірністю. Однак в силу того, що ці

імовірності залежать від ключа — необхідно знати ключ, щоб знайти диференціали з високою імовірністю для побудови атаки, що знаходить такий ключ. У такому випадку ми вважаємо, що розподіли при різних значеннях ключа приблизно однакові. Тому для оцінки складності проведення диференціальної атаки будемо використовувати середню імовірність диференціалу

$$EDP_{\oplus}^{f_k}(\alpha,\beta) = \frac{1}{2^n}\sum_{k\in K} DP_{\oplus}^{f_k}(\alpha,\beta)$$

Таким чином, гарантована складність проведення атаки визначається максимумом середньої імовірності диференціалу:

$$MEDP_{\oplus}(f_k) = \max_{\alpha,\beta\neq 0} EDP_{\oplus}^{f_k}(\alpha,\beta)$$

цей параметр є основною чисельною характеристикою, що визначає стійкість криптографічних перетворень до диференціального криптоаналізу.

Л.В. Ковальчук [4] запропонувала поняття *середньої за ключами імовірності диференціалу шифруючого перетворення f_k у точці x*, що є досить зручним для побудови оцінок значення $MEDP$:

$$DP_{\oplus}^{f_k}(x,\alpha,\beta) = \frac{1}{2^n}\sum_{k\in K}[f_k(x\oplus\alpha) = f_k(x)\oplus\beta].$$

Максимумом середньої за ключами імовірністю диференціалу називається величина:

$$MDP_{\oplus}(f_k) = \max_{\alpha,\beta,x\neq 0} DP_{\oplus}^{f_k}(x,\alpha,\beta).$$

Середнє значення середньої за ключами імовірності диференціалу - це усереднена за входми x сума імовірностей диференціалів:

$$EDP_{\oplus}^{f_k}(\alpha,\beta) = \frac{1}{2^n}\sum_{x\in V_n} DP_{\oplus}^{f_k}(x,\alpha,\beta).$$

Для оцінювання гарантованої складності проведення диференцальних криптоатак можна використовувати верхні оцінки для MDP, оскільки очевидно, що $MDP \geq MEDP$. Слід зазначити, що MDP зазвичай простіше обчислюється.

Шифруюче перетворення f_k називається *марковсъким* (відносно операції $\oplus$), якщо для будь-якого значення x виконується рівність:

$$DP_{\oplus}^{f_k}(x, \alpha, \beta) = DP_{\oplus}(0, \alpha, \beta),$$

тобто для марковських перетворень значення середніх за ключами диференціальних імовірностей не залежать від точки входу. Звідси випливає, що для марковського перетворення вірна наступна рівність:

$$DP_{\oplus}^{f_k}(x, \alpha, \beta) = EDP_{\oplus}^{f_k}(\alpha, \beta),$$

таким чином можна нехтувати параметром x при побудові аналітичних оцінок стійкості до диференціальних криптоатак.

Нехай E — ітеративний $r-$раундовий блоковий шифр.

Диференціальною характеристикою шифру E називають послідовніть бітових векторів $\Omega = (\omega_0, ..., \omega_r)$, де $\omega_i \in V_q \setminus \{0\}$. Ця характеристика розглядається як послідовність змін даних між раундами протягом шифрування: якщо подати на вхід повідомлення X_0 та $X_0^{'}$ такі, що $X_0 = \omega \oplus X_0^{'}$, то ми отримаємо $X_1 = \omega \oplus X_1^{'}$, ..., $X_r = \omega \oplus X_r^{'}$.

Середньою за ключами імовірністю диференціальної характеристики Ω шифру E у точці X_0 називається така величина:

$$DP_{\oplus}^{E}(\Omega, X_0) = \overline{\sum_{k_1 \in K}} \dots \overline{\sum_{k_r \in K}} \prod_{i=1}^{r} \left[f_{k_i}^{(i)}(X_{i-1}) \oplus \omega_{i-1} = \omega_i \oplus f_{k_i}^{(i)}(X_{i-1}) \right], \quad (1.1)$$

де $\overline{\sum}_{k \in K}$ — усереднена сума за елементами $k \in K$.

Якщо в ітеративному r-раундовому блоковому шифрі E кожне раундове перетворення є марковським (відносно $\oplus$), тоді виконується наступна рівність:

$$DP^{E}(\Omega, X_0) = \prod_{i=1}^{r} EDP^{f_{k_i}^{(i)}}(\omega_{i-1}, \omega_i). \quad (1.2)$$

Тобто обчислення імовірностей диференціальних характеристик для марковських шифрів зводиться до оцінювання диференціалів окремих раундів.

1.3 Лінійний криптоаналіз

Лінійний криптоаналіз це атака з використанням відомого відкритого тексту, яка намагається використовувати високоймовірні появи лінійних виразів, які включають біти відкритого тексту, шифрованого тексту та підключей.

Розглянемо формальну теорію стійкості до лінійного криптоаналізу.

Нехай $f : V_n \to V_n$. *Коефіцієнтом кореляції* називається така величина:

$$C_f(\alpha,\beta) = \frac{1}{2^n} \sum_{x \in V_n} (-1)^{\alpha \cdot x \oplus \beta \cdot f(x)}.$$

Величина, що визначає стійкість шифру до атак збоку лінійного криптоаналізу, називається *лінійним потенціалом*. Даний параметр є квадратом коефіцієнта кореляції й записується таким чином:

$$LP^f(\alpha,\beta) = (C_f(\alpha,\beta))^2.$$

Складність атаки є обернено пропорційною до значення цієї величини.

Максимальним лінійним потенціалом називається така величина:

$$MLP(f) = \max_{\alpha,\beta \neq 0} LP^f(\alpha,\beta).$$

Даний параметр є основною чисельною характеристикою, що визначає гарантовану стійкість шифру до лінійного криптоаналізу у випадку, коли ми досліджуємо перетворення, що не залежать від ключа, оскільки мінімальна складність атаки буде обернено пропорційна до неї.

Нехай $f_k : V_n \times K \to V_n$, $k \in K$, K – ключовий простір, $y = f_k(x)$, $K = V_l$. *Усереднений лінійний потенціал* визначається таким чином:

$$ELP^{f_k}(\alpha,\beta) = \frac{1}{2^l} \sum_{k \in K} LP_k^f(\alpha,\beta).$$

Це величина, яку ми досліджуємо при розляданні ключезалежних перетворень. Даний параметр характеризує стійкість шифру до лінійних криптоатак.

Відповідно, гарантована складність проведення атаки визначається максимумом середнього лінійного потенціалу. *Максимум середнього лінійного потенціалу* визначається таким чином:

$$MELP(f_k) = \max_{\alpha,\beta\neq 0} ELP^{f_k}(\alpha,\beta).$$

Наведений вище параметр є основною чисельною характеристикою, що визначає стійкість шифру до лінійного криптоаналізу у випадку, коли ми досліджуємо ключезалежні перетворення, оскільки мінімальна складність атаки буде обернено пропорційна до неї.

Якщо раундова функція $f_k(x) = g(x \oplus k)$, то $\forall\alpha\forall\beta$ справедливим є наступне твердження:

$$ELP^{f_k}(\alpha,\beta) = LP^g(\alpha,\beta)$$

Лінійною характеристикою шифру E називають послідовніть бітових векторів $\Omega = (\omega_0, ..., \omega_r)$, де $\omega_i \in V_q \setminus \{0\}$. Кожні два сусідні вектори розглядаються як певна лінійна апроксимація раундової функції.

Нехай $E_k(x) = F^{(r)}_{k_r}(\dots F^{(1)}_{k_1}(x))$, $F^{(i)}_{k_i}(x) = f_i(x \oplus k_i)$, тоді справедливим є наступне твердження:

$$ELP^{E_k}(\alpha,\beta) = \sum_{\Omega\in\Omega(\alpha,\beta)} ELCP^{E_k}(\Omega), \tag{1.3}$$

де

$$ELCP^{E_k}(\Omega) = \prod_{i=1}^{r} ELP^{f_i}(\omega_{i-1},\omega_i).$$

1.4 Теоретичні оцінки стійкості Фейстель-подібних схем до диференціального та лінійного криптоаналізу

У цьому розділі буде розглянуто існуючі теоретичні оцінки стійкості Фейстель-подібних схем з точки зору диференціального та лінійного криптоаналізу.

У 1995 році Кайса Нюберг (Kaisa Nyberg) та Ларс Кнудсен (Lars Knudsen) [5] сформулювали задачу доведення стійкості блокових шифрів до диференціального криптоаналізу саме у тих термінах, які було розлянуто в 1.2. Ними було розв'язано цю задачу для класичної схеми Фейстеля.

Нехай DES-подібна схема Фейстеля — це схема Фейстеля, в якій раундові функції мають такий вигляд: $f_k = g(x \oplus k)$.

Розглянемо чотирираундову DES-подібну схему Фейстеля $E = \Phi[f_1,f_2,f_3,f_4]$. Якщо $p = \max\limits_i MDP_{\oplus}(f_i)$ - максимальна імовірність диференціалів по всіх раундових функціях. Тоді максимальна ймовірність диференціалів такого шифру $MDP_{\oplus}(E) \leq 2p^2$.

Така оцінка справедлива для 4-раундової схеми з довільними раундовими функціями. Але якщо f_i - бієктивні, то така оцінка досягається за три раунди, а не за чотири.

У 1996 році Аокі (Aoki) та Ота (Ohta) [6] показали, що твердження теореми Ніберг та Кнудсена можна підсилити.

Розглянемо трьохраундову схему Фейстеля $E = \Phi[f_1,f_2,f_3]$, f_i-бієктивні фунції. Якщо $p = \max\limits_i MDP_{\oplus}(f_i)$ - максимальна імовірність диференціалів по всіх раундових функціях, що у нас є. Тоді максимальна ймовірність диференціалів такого шифру $MDP_{\oplus}(E) \leq p^2$. В свою чергу Кайса Нюберг у своїй статті [7] показала, що якщо $q = \max\limits_i MLP(f_i)$ — максимальний лінійний потенціал, то для трьох раундів схеми Фейстеля $MLP(E) \leq q^2$.

Брюс Шнейер та Джон Келсі у своїй статті [3] про дослідження незбалансованих схем Фейстеля стверджують, що як правило диференціальний криптоаналіз становиться тим важчий, чим більший коефіцієнт розсіювання R_d, тобто незбалансовані схеми Фейстеля при збільшенні s по відношенню до t стають більш стійкими до диференціальних атак.

Водночас стійкість до лінійного криптоаналізу напряму залежить від коефіцієнту плутаниці R_c, саме тому коли t збільшується по відношеню до

s – проводити лінійні криптоатаки стає набагото складніше.

Також Шнейер і Келсі відзначають, що незбалансовані схеми Фейстеля можуть давати виграш як у плані ефективності, так і в плані стійкості до відомих методів криптоаналізу; проте сучасний математичний апарат не дозволяє отримувати аналітичні та практичні оцінки стійкості.

У той же час такі питання по незбалансованим схемам залишаються відкритими:

1) чи можна використовувати раундові функції f для забезпечення деякого опору до лінійних криптоатак і водночас структуру незбалансованих схем Фейстеля для забезбечення деякого опору до диференціальних криптоатак?

2) чи мають неповні незбалансовані схеми Фейстеля переваги над повними?

3) чи є розумним чергувати декілька раундів джерельноважких незбалансованих схем Фейстеля для опору диференціальним криптоатакам, а далі - декілька раундів незбалансованої схеми Фейстеля для опору лінійним криптоатакам?

У 1997 році Міцуру Мацуї отримав теоретичні оцінки стійкості для збалансованої схеми MISTY.

Розглянемо трьохраундову схему Фейстеля $E = \Phi[f_1,f_2,f_3]$, де f_i-бієктивні фунції.Якщо $p = \max\limits_i MDP_{\oplus}(f_i)$ — максимальна імовірність диференціалів по всіх раундових функціях наведеної вище схеми. Тоді максимальна ймовірність диференціалів такого шифру $MDP_{\oplus} \leq p^2$. Міцуру Мацуї було отримано аналогічний результат для схеми MISTY.

А для незбалансованої неоднорідної трираундової схеми MISTY Міцуру Мацуї [8] отримав теоретичні оцінки стійкості як з точки зору лінійного, так і диференціального криптоаналізу:

$$MDP_{\oplus}(E) \leq \max\{MDP_{\oplus}(f_1)MDP_{\oplus}(f_2), MDP_{\oplus}(f_2)MDP_{\oplus}(f_3), 2^{m-n}MDP_{\oplus}(f_1)MDP_{\oplus}(f_3)\}.$$

$$MLP(E) \leq \max\{MLP(f_1)MLP(f_2), MLP(f_2)MLP(f_3), 2^{m-n}MLP(f_1)MLP(f_3)\},$$

де n, m - бітова довжина лівого та правого блоку відповідно, $n \leq m$, f_i - бієктивні для довільного ключа.

Згодом оцінки Мацуї ним же були узагальнені для іншої незбалансованої схеми — R-схеми, а також для їх немарковських варіантів.

У роботі [9] було досліджено неоднорідну незбалансовану схему Фейстеля, в основі якої лежить використання бієктивних раундових перетворень, і яка для перемішування частин вхідного блоку між собою використовувала додаткові лінійні перетворенння (звужуючі та розширюючі). В залежності від їх використання до чи після нелінійної раундової функції, розглядались два різних варіанти неоднорідних схем.

В цій роботі було показано, що для першого випадку схема являється абсолютно нестійкою до лінійного криптоаналізу, в одночас оцінки стійкості такої схеми до диференціального криптоаналізу значно гірші за відповідні оцінки для L- та R-схем. Для іншого варіанта схеми було встановлено, що вона є нестійкою з точки зору диференціальних криптоатак, а також що оцінки стійкості до лінійного криптоаналізу аналітично не будуються. Таким чином, в результаті було показано, що неоднорідні незбалансовані схеми Фейстеля не є криптографічно стійкими.

Однак серед існуючих теоретичних оцінок стійкості до лінійного та диференціального криптоаналізу, не вдається знайти результати чи міркування щодо однорідної незбалансованої схеми MISTY. Тому можна зробити висновок, що ще не було опубліковано досліджень зазначеної схеми.

Висновки до розділу 1

У даному розділі було розглянуто поняття ітеративного блокового шифру, основні види Фейстель-подібних схем, основні положення диференціального та лінійного криптоаналізу. Також розглянуто деякі існуючі теоретичні оцінки стійкості Фейстель-подібних схем до диференціального та лінійного криптоаналізу.

Було показано, що на відміну від звичайних схем Фейстеля, неоднорідних Фейстель-подібних схем таких як незбалансована неоднорідна трираундова схема MISTY, схема Фейстеля та інших шифрів, не було опубліковано досліджень однорідної незбалансованої схеми MISTY.

2 ЕКСПЕРИМЕНТАЛЬНІ ОЦІНКИ СТІЙКОСТІ ОДНОРІДНОЇ НЕЗБАЛАНСОВАНОЇ СХЕМИ MISTY ДО ДИФЕРЕНЦІАЛЬНОГО ТА ЛІНІЙНОГО КРИПТОАНАЛІЗУ

Другий розділ присвячено дослідженню стійкості однорідної незбалансованої схеми MISTY до атак збоку диференціального та лінійного криптоаналізу, а також встановленню того, наскільки лінійна частина впливає на стійкість в шифрах такого виду.

2.1 Опис експерименту

У подальшому розглядається п'ятибітова однорідна незбалансована важкоцільова (target heavy) схема MISTY, кожне раундове перетворення якої схематично зображено на рис. 2.1.

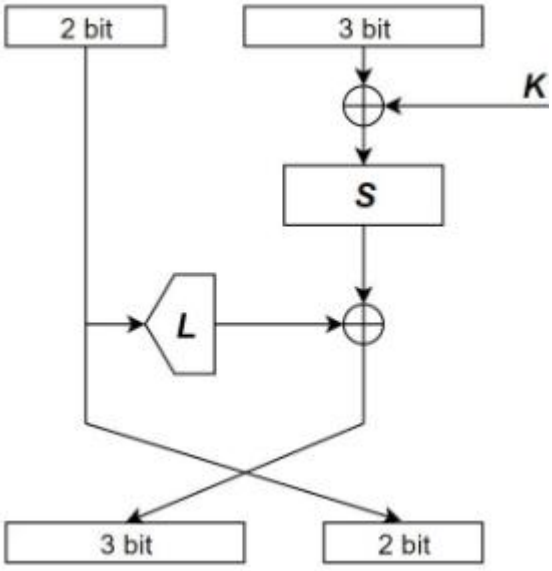

Рисунок 2.1 – Один раунд незбалансованої схеми MISTY

У наведеній схемі вхідний блок даних розбивається на дві нерівні частини: джерельний блок — 2 біти, цільовий блок — 3 біти відповідно.

Нехай x, y – значення джерельного і цільового блоку відповідно. Тоді раундова функція цієї схеми виглядає таким чином:

$$F_k(x, y) = (L(x) \oplus S(y \oplus k), x),$$

де k – ключ першого раунду, S – S-блок (блок підстановок), у данному випадку є функцією виду $S : V_3 \to V_3$, L – лінійна функція виду $L : V_2 \to V_3$, яка задається матрицею 3×2, ранг якої дорівнює 2. Тобто функція L представляє собою розширююче перетвореня, що дозволяє змішувати двохбітні вектори з троьхбітними.

Для розрахунків ми беремо 5-бітовий вхідний блок, оскільки доступні обчислювальні можливості не дозволяють обчислити необхідні параметри стійкості; однак для малого розміру параметри стійкості легко рахуються перебором.

Було обрано важкоцільову схему, тому що вона виглядає більш перспективно з точки зору застосування на практиці, оскільки стверджується, що схеми такого виду теоретично є більш стійкими до атак збоку диференціального та лінійного криптоаналізу.

Основною задачею є зрозуміти поведінку імовірності диференціалів та лінійних потенціалів в шифрах такого виду, а також зрозуміти, наскільки лінійна частина впливає на цю поведінку.

Для цього ми спочатку для двох обраних S-блоків оцінюємо їх розподіли MDP досліджуваною схеми протягом декількох раундів, намагаючись розпізнати деяку закономірність.

Далі обираємо такі функції L, які є кращими з точки зору стійкості до диференціального криптоаналізу в найгіршому випадку, тобто для всіх S-блоків з фіксованою лінійною функцією L ми будемо мати верхню границю для MDP — це і буде найнижча верхня границя із усіх можливих.

На наступному етапі обираємо такі функції L, які є кращими з точки зору стійкості до лінійного криптоаналізу в найгіршому випадку, тобто для всіх S-блоків з фіксованою лінійною функцією L ми будемо

мати верхню границю для $MELP$ — це і буде найнижча верхня границя із усіх можливих.

Після проведення описаних вище досліджень ми дізнаємось, чи співпадають кращі функції L з точки зору стікості до лінійного та диференціального криптоаналізу.

2.2 Дослідження розподілів ймовірностей диференціалів схеми, яка досліджується

Нехай $\alpha = (\alpha_x, \alpha_y)$, $\beta = (\beta_x, \beta_y)$ – вхідна і вихідна різниця відповідно. Використовуючи описаний у розділі 1.2 математичний апарат формальної теорії диференціального криптоаналізу можна одержати такий вираз для імовірності диференціалів раундової функції F через імовірності диференціалів S-блоку S:

$$DP^{F_k}(\alpha, \beta) = [\alpha_x = \beta_x]\, DP^S(\alpha_y, \beta_y \oplus L(\alpha_x)),$$

де DP^S – відповідна диференціальна ймовірність S-блоку.

Доведення. Розглянемо похідну за напрямком α для фунцкії F_k, маємо:

$$\begin{aligned} &F_k(x \oplus \alpha_x, y \oplus \alpha_y) \oplus F_k(x, y) = \\ &\quad = (L(x) \oplus L(\alpha_x) \oplus S(y \oplus \alpha_y \oplus k), x \oplus \alpha_x) \oplus (L(x) \oplus S(y \oplus k), x) = \\ &\qquad\qquad = (L(\alpha_x) \oplus S(y \oplus \alpha_y \oplus k) \oplus S(y \oplus k), \alpha_x) = (\beta_y, \beta_x). \end{aligned}$$

За означенням імовірності диференціалів раундової функції F,

$$DP^{F_k}(\alpha, \beta) = \overline{\sum_k}[\alpha_x = \beta_x][S(y \oplus \alpha_y \oplus k) \oplus S(y \oplus k) = \beta_y \oplus L(\alpha_x)],$$

введемо заміну $y \oplus k = u$, отримуємо:

$$DP^{F_k}(\alpha, \beta) = \overline{\sum_u}[\alpha_x = \beta_x][S(u \oplus \alpha_y) \oplus S(u) = \beta_y \oplus L(\alpha_x)],$$

відповідно, маємо такий результат:

$$DP^{F_k}(\alpha, \beta) = [\alpha_x = \beta_x] DP^S(\alpha_y, \beta_y \oplus L(\alpha_x)).$$

Бачимо, що $DP^{F_k}(\alpha, \beta)$ не залежить від x та y. Таким чином, робимо виснок, що шифруюче перетворення F_k — марковське відносно операції $\oplus$. □

Нехай $G_{k_1,k_2}(x, y) = F^{(1)}_{k_1}(F^{(2)}_{k_2}(x, y))$ – функція, яка описує два раунди нашої схеми; диференціальні імовірність для функції G обчислюється за такою формулою [10]:

$$DP^G(\alpha, \beta) = \sum_{\gamma} DP^{F^{(2)}}(\alpha, \gamma) \cdot DP^{F^{(1)}}(\gamma, \beta).$$

Дане співвідношення безпосередньо випливає з формули 1.2.

Позначимо $H_{k_1,k_2,k_3}(x, y) = F^{(3)}_{k_3}(F^{(2)}_{k_2}(F^{(1)}_{k_1}(x, y)))$ як функцію, яка описує три раунди нашої схеми. У такому випадку диференціальна ймовірність для функції H обчислюється за такою формулою:

$$DP^H(\alpha, \beta) = \sum_{\gamma} DP^G(\alpha, \gamma) \cdot DP^{F^{(3)}}(\gamma, \beta).$$

Аналогічним чином можна отримати формули для обчислення диференціальної ймовірності функції від будь-якої кількості раундів.

Наведемо основні кроки наших експериментальних обчислень. Спочатку було проведено генерування всіх можливих функцій L ранг яких становить 2, загальна кількість таких функцій становить 42. Також було згенеровано всі можливі S-блоки бітової довжини 3; загальна кількість таких блоків перестановок становить $(2^n)!$, де n - кількість бітів на вході S-блока. У нашому випадку, загальна їх кількість становить $(2^3)! = 40320$.

Наступним кроком було відкинуто найгірші з точки зору диференціального криптоаналізу (ті, на які можна легко провести атаку) S-блоки, тобто ті, для яких $MDP^S = 1$. Кількість S-блоків, для яких $MDP^S = 1$ становить 10752. Отже, після фільтрації залишилось усього 29568 S-блоків, для яких $MDP^S \neq 1$.

Дослідження максимумів диференціальних імовірностей для фіксованих S-блоків

На першому етапі дослідження було обрано декілька S-блоків для подальшого підрахування максимальної диференціальної ймовірності

функції, яка описує r раундів нашої схеми для кожної із всіх можливих функцій L.

Для зручності будемо позначати досліджуваний S-блок як набір елементів $[a_0, a_1, ..., a_{2^n-1}]$, такий, що $a_i = S(i)$, n – кількість бітів на вході S-блоку.

Розглянемо S-блок $[0, 1, 2, 4, 3, 6, 5, 7]$. Для даного блоку підстановок і всіх можливих функцій L було отримано розподіл максимумів диференціальної ймовірності, який наведено для 3-раундової схеми на рис. 2.2, для 4-раундової схеми на рис. 2.3, та для 5-раундової схеми на рис. 2.4, відповідно. Горизонтальна вісь – значення MPD, вертикальна – кількість лінійних функцій L, яким відповідає значення MPD.

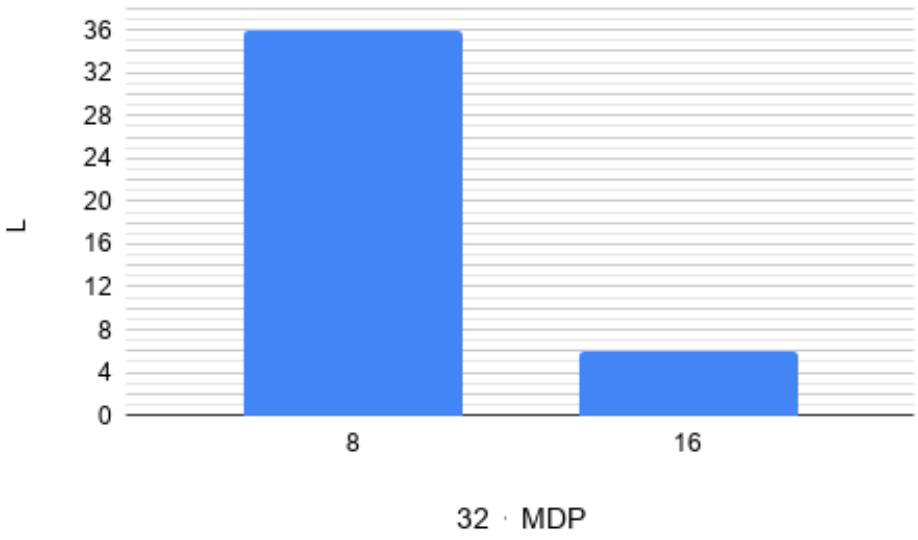

Рисунок 2.2 – Розподіл значень $2^5 \cdot MDP$ для схеми з трьома раундами для першого S-блоку.

Для порівняння, розглянемо S-блок $[0, 1, 2, 3, 4, 6, 7, 5]$. Слід зазначити, що наведений S-блок та попередньо досліджуваний мають доволі схожі розподіли диференціальних ймовірностей, також вони мають однакове значення MDP^s. По аналогії до попереднього блоку перестановок, для обраного S-блоку і всіх можливих функцій L також було отримано розподіл максимумів диференціальної ймовірності, який

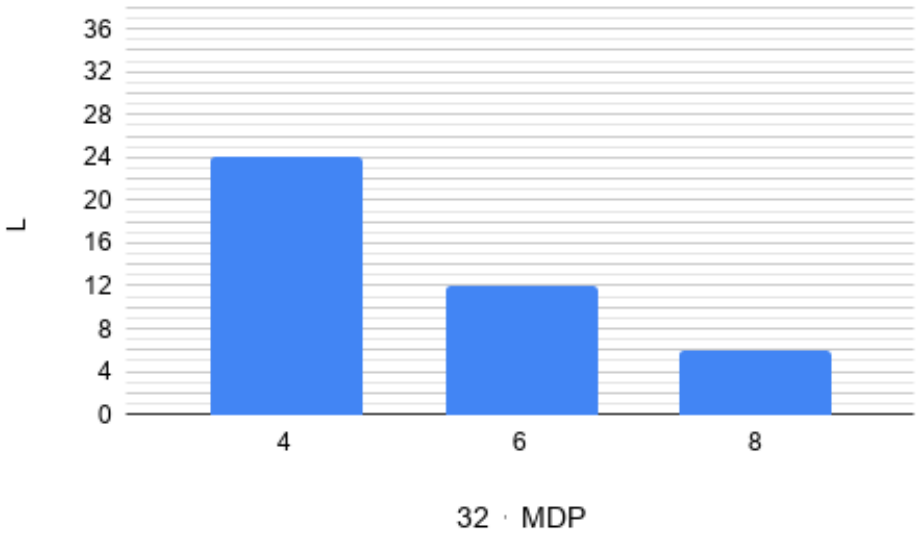

Рисунок 2.3 – Розподіл значень $2^5 \cdot MDP$ для схеми з чотирма раундами для першого S-блоку

наведено для 4-раундової схеми на рис. 2.5, та для 5-раундової схеми на рис. 2.6, відповідно.

З гістограми для трираундової схеми випливає, що для першого S-блоку 36 лінійних перетворень приймають значення $MDP = 0.25$ та для шістьох функцій L максимальна диференціальна ймовірність дорівнює 0.5, що є незначною перевагою для другого S-блоку над першим, оскільки для другого блоку перестановок при всіх лінійних перетвореннях значення $MDP = 0.25$. Але на гістограмах для п'ятираундових схем бачимо, що другий S-блок має набагато більше різноманітних максимумів, у порівнянні до першого: у ньому різноманітність досить низька. Слід звернути увагу також на те, що для пятираундової схеми при другому S-блоку максимальне значення MDP є більшим, ніж для аналогічної схеми при першому блоку перестановок, хоча для трираундової схеми — навпаки.

Опираючись на отримані результати, можна зробити висновок, що для приблизно однакових S-блоків поведінка досліджуваної незбалансованої схеми MISTY неоднозначна, оскільки при деяких функціях L спостерігаються досить низькі показники MPD, а при інших

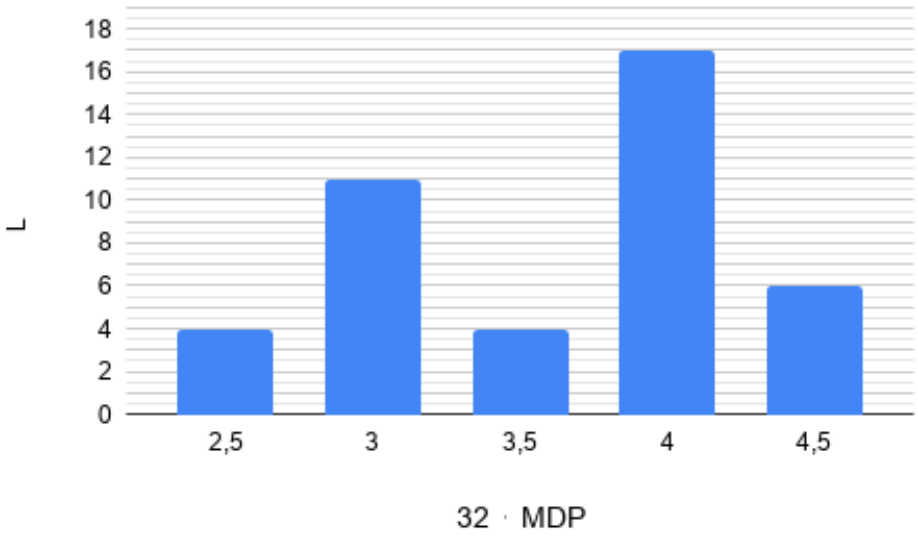

Рисунок 2.4 – Розподіл значень $2^5 \cdot MDP$ для схеми з пятьма раундами для першого S-блоку

— навпаки, великі значення.

При дослідженні однорідної незабалансованої схеми MISTY експериментальним шляхом було виявлено, що маніпулювання окремими складовими незбалансованої фейстель-подібної схеми такими як S-блок та лінійна функція може привести як до збільшення стійкості системи до диференціального криптоаналізу, так і до її зменшення. Одержані розрахункові результати показують, що для різних лінійних функцій L та для різної кількості раундів поведінка диференціальних імовірностей неоднозначна.

Дослідження розподілів MDP в залежності від лінійної функції

На наступному етапі для кожної із 42 можливих функцій L було підраховано максимальні диференціальні ймовірності функції, яка описує r раундів нашої схеми для кожного із 29568 S-блоків й було обрано мінімальне значення MDP^F. Тобто ми будемо мати верхню межу для MDP^F — це і буде верхньою границею із усіх можливих випадків. Іншими словами, ми будемо оцінювати найкращій із усіх найгірших випадків з точки зору стійкості до диференціального криптоаналізу для

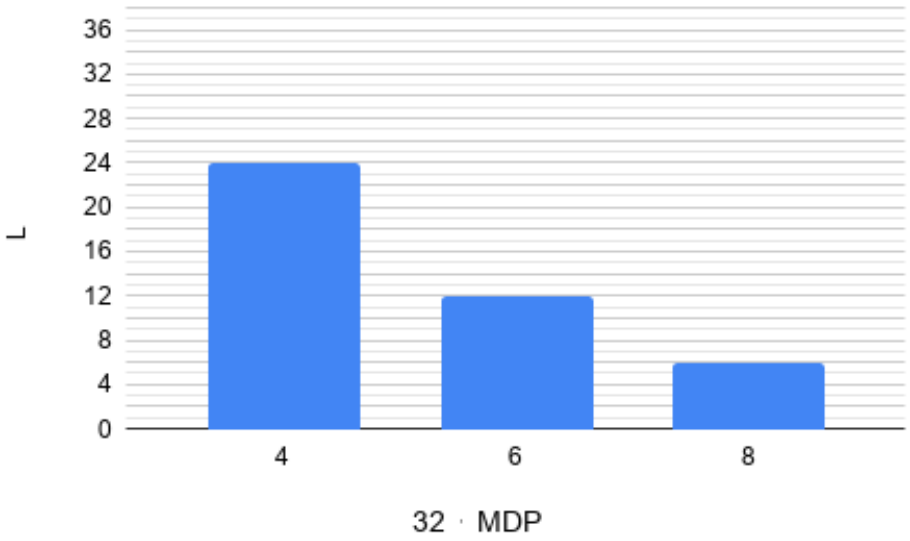

Рисунок 2.5 – Розподіл значень $2^5 \cdot MDP$ для схеми з чотирма раундами для другого S-блоку

кожної із згенерованих функцій L.

Отримані розподіли верхніх оцінок для кожної L наведено для 4-раундової схеми на рис. 2.7, для 5-раундової схеми на рис. 2.8, для 6-раундової схеми на рис. 2.9 та для 7-раундової схеми на рис. 2.10, відповідно. Горизонтальна вісь показує номер досліджуваної функції L , вертикальна – мінімальне значення MDP^F при функції L серед усіх S-блоків.

Розглянемо гістограму для чотирираундової схеми. Серед усіх можливих функцій L виділяються функції під номером 15, 16, 17, 18 та 37, 38, 39, 40, для яких верхня межа $MDP = 0.3125$, що суттєво меньше за верхні оцінки для всіх інших функцій, для яких верхня межа $MDP = 0.5$.

Розглянемо гістограму для пятираундової схеми. Як і в гістограмі для чотирираундової схеми — найбільше виділяються функції під номером 15, 16, 17, 18 та 37, 38, 39, 40, для яких верхня межа $MDP = 0.25$ на фоні тих фунцій з верхньою межею $MDP = 0.3175$ (це функції 1-10, 19-20, 25-26, 31-32) $MDP = 0.3125$ (це функції 11-14, 21-24, 27-30, 33-36).

Розглянемо гістограму для шестираундової схеми. Як і в гістограмі

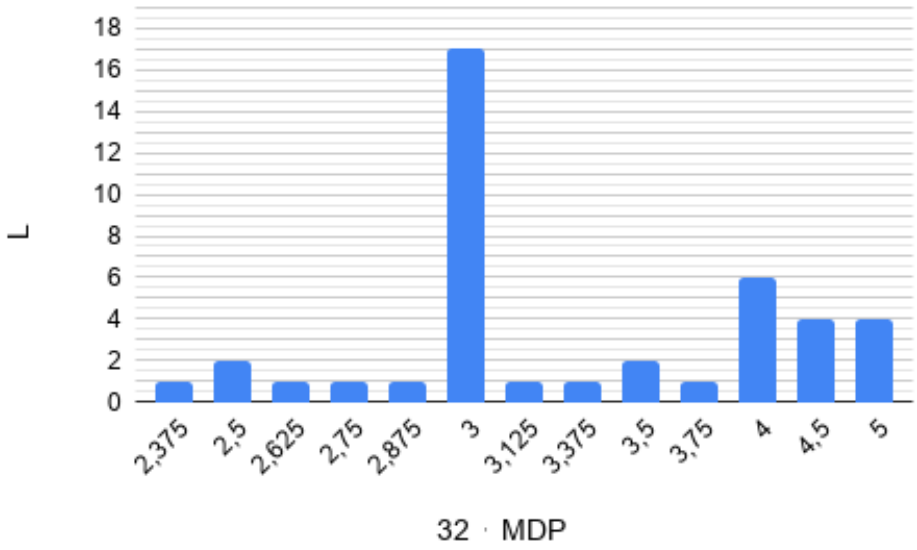

Рисунок 2.6 – Розподіл значень $2^5 \cdot MDP$ для схеми з пятьма раундами для другого S-блоку

для п'яти та чотирьох раундової схеми — найкращі показники MDP мають функції під номером 15, 16, 17, 18 та 37, 38, 39, 40, для яких верхня межа $MDP = 0.21875$. Також слід звернути увагу на функції під номером 3-4, 7-8, 41-42, для яких значення верхніх оцінок MDP стрімко знизилися у порівнянні до попереднього раунду — для них значення $MDP = 0.25$. Для всіх інший лінійних функцій показники верхніх оцінок або не суттєво зменшились, або не змінились взагалі.

З відомостей наведених на гістограмі для 7-раундової досліджуваної схеми, можна зробити висновок, що тенденція зберігається: знову найкращі показники MDP мають функції під номером 15, 16, 17, 18 та 37, 38, 39, 40; у сьомому раунді для ціх функцій верхня межа $MDP = 0.1875$, що значно краще ніж показники для всіх інших функцій, оскільки для них показники верхніх оцінок у порінянні до шостого раунда не змінились взагалі.

Із аналізу розподілів верхніх оцінок MDP для всіх S-блоків при кожній із функції L було встановлено, що найкращі верхні границі MDP було отримано при функціях L під номером 15, 16, 17, 18 та 37, 38, 39, 40.

Будемо позначати матриці як L_i, де i — номер лінійної функції L. Випишемо матриці, яким відповідають функції L з найкращими верхніми

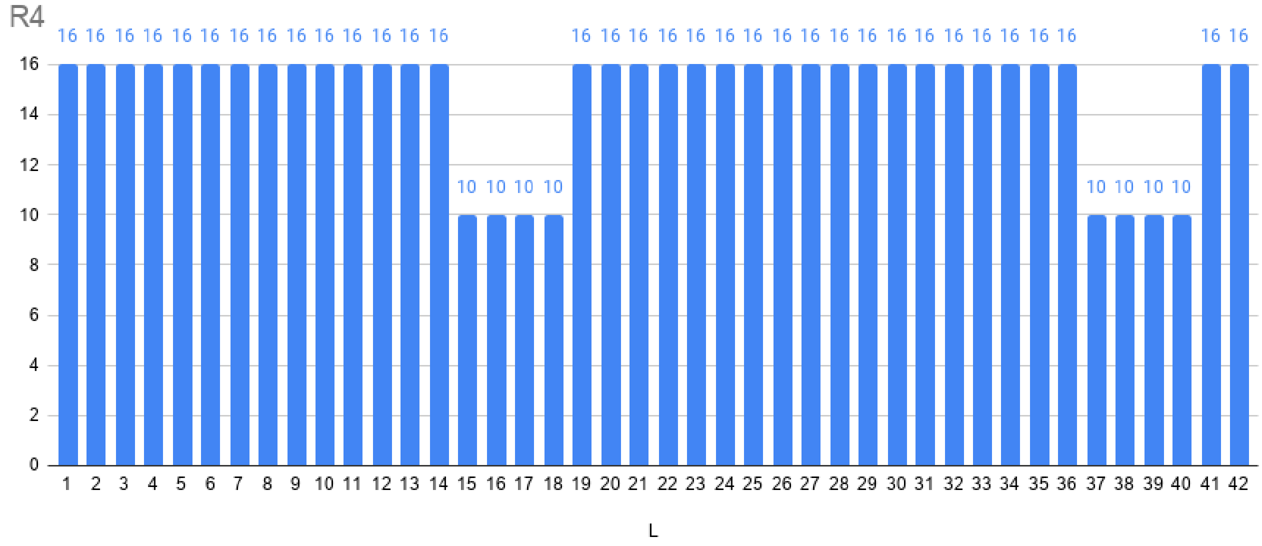

Рисунок 2.7 – Розподіл значень $2^5 \cdot MDP$ для схеми з чотирма раундами для кожної L

оцінками:

$$L_{15} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} L_{16} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} L_{17} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} L_{18} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$L_{37} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} L_{38} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} L_{39} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} L_{40} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Первинний аналіз отриманих функцій L показав, що серед матриць, які відповідають цим функціям, не присутні явні особливості, які підсилюють стійкість схеми до диференціального криптоаналізу. Відповідно, скоріше за все отримані результати не можна аналітично промасштабувати для схем з більшою кількістю біт у вхідному блоці даних, оскільки не зрозуміло як повинні виглядати матриці для великих схем.

Слід зауважити, що для деякого конкретного S-блока та лінійної

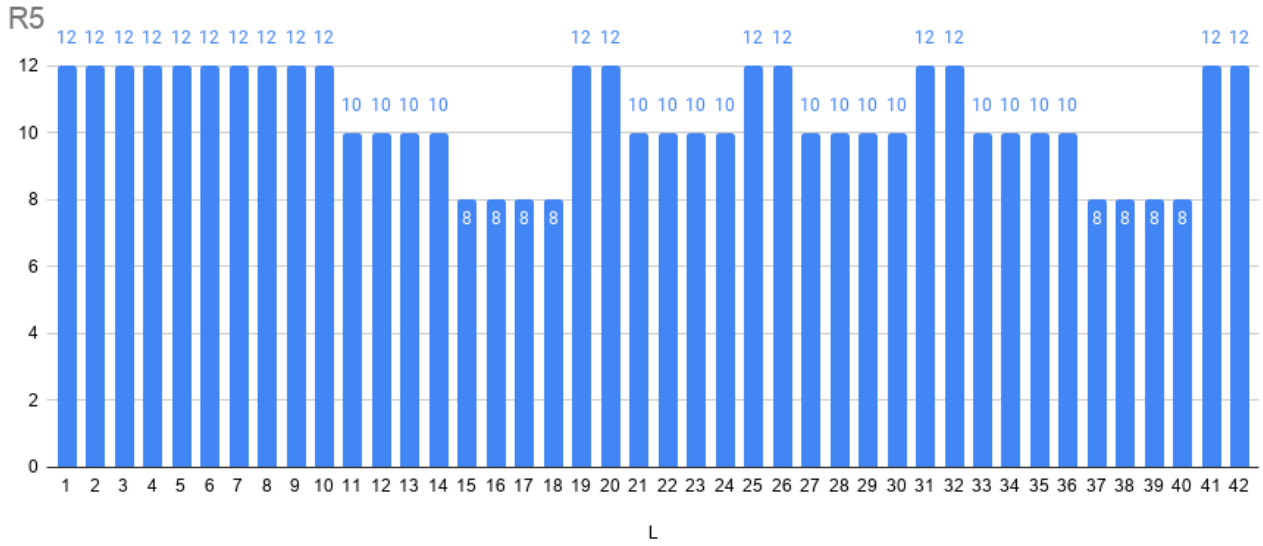

Рисунок 2.8 – Розподіл значень $2^5 \cdot MDP$ для схеми з пятьма раундами для кожної L

функції, яка не є серед наведених вище (йдеться про кращі L), значення параметра MDP шифру може бути й нижчим. Проте, якщо не відомо, який S-блок використовується у досліджуваній схемі, функції L під номером 15, 16, 17, 18 та 37, 38, 39, 40 дають гарантовану стійкість до диференціального криптоаналізу, оскільки для будь-якого S-блока при таких функціях показник MDP шифру буде мати нетривіальну фіксовану верхню межу.

2.3 Дослідження розподілів лінійних потенціалів схеми, яка досліджується

Нехай $\alpha = (\alpha_x, \alpha_y)$, $\beta = (\beta_y, \beta_x)$ – вхідна і вихідна різниця відповідно, тут x означає 2 біти, y означає 3 біти. Використовуючи описаний у розділі 1.3 математичний апарат формальної теорії лінійного криптоаналізу можна одержати такий вираз для усередненого лінійного потенціалу раундової функції F через лінійний потенціал S-блока:

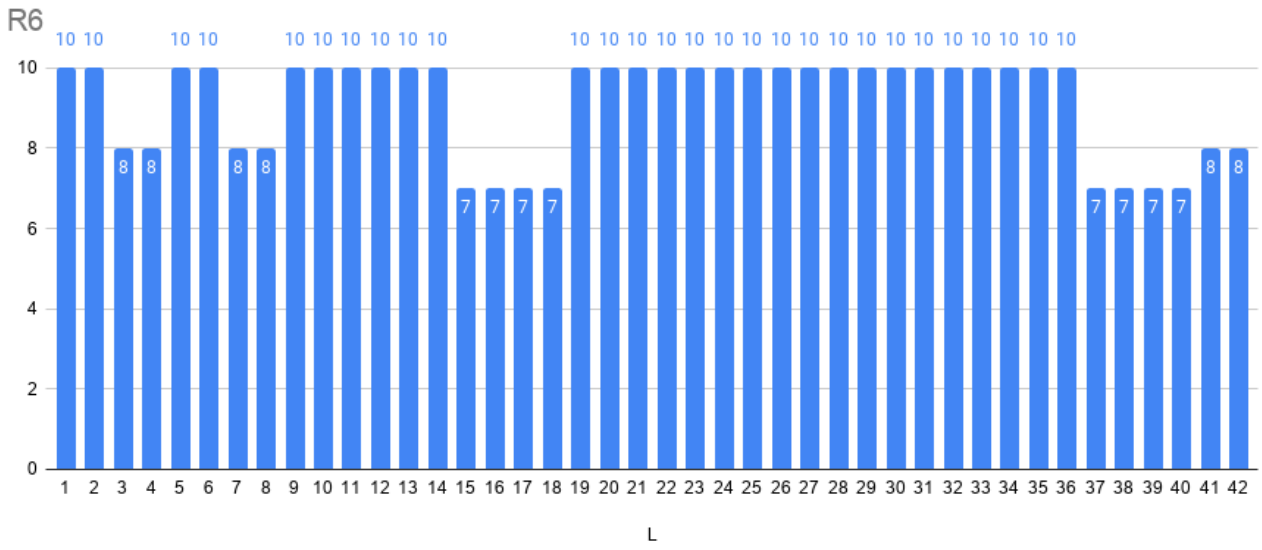

Рисунок 2.9 – Розподіл значень $2^5 \cdot MDP$ для схеми з шістьома раундами для кожної L

$$ELP^{F_k}(\alpha,\beta) = \overline{\sum_x}[\alpha_x = \beta_x \oplus L^*(\beta_y)]LP^S(\alpha_y,\beta_y),$$

де LP^S – відповідний лінійний потенціал S-блоку, L^* — спряжена матриця.

Доведення.

За означенням усередненого лінійного потенціалу:

$$ELP^{F_k}(\alpha,\beta) = \overline{\sum_k}\left(\overline{\sum_{x,y}}(-1)^{\alpha\cdot(x,y)\oplus\beta\cdot F_k(x,y)}\right)^2 =$$

$$= \overline{\sum_k}\left(\overline{\sum_{x,y}}(-1)^{\alpha_x\cdot x\oplus\alpha_y\cdot y\oplus\beta_y\cdot(L(x)\oplus S(y\oplus k))\oplus\beta_x\cdot x}\right)^2 =$$

$$= \overline{\sum_k}\left(\overline{\sum_{x,y}}(-1)^{x\cdot(\alpha_x\oplus\beta_x\oplus L^*(\beta_y))}(-1)^{\alpha_y\cdot y\oplus\beta_y\cdot S(y\oplus k)}\right)^2 =$$

$$= [\alpha_x \oplus \beta_x \oplus L^*(\beta_y)]\overline{\sum_k}\left(\overline{\sum_y}(-1)^{\alpha_y\cdot y\oplus\beta_y\cdot S(y\oplus k)}\right)^2.$$

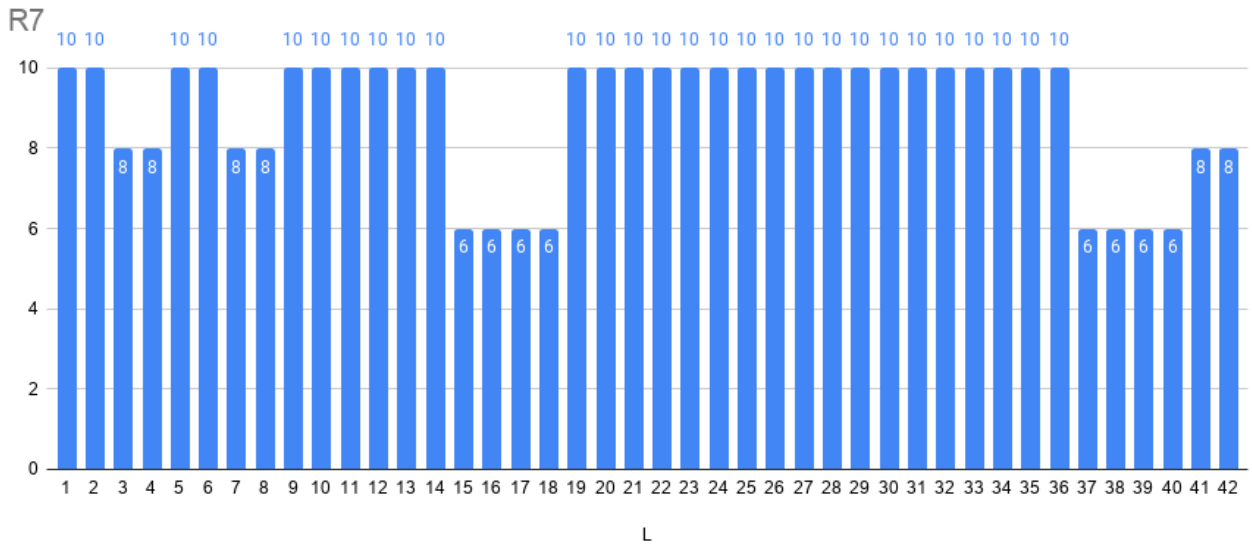

Рисунок 2.10 – Розподіл значень $2^5 \cdot MDP$ для схеми з сімома раундами для кожної L

Введемо заміну $u = y \oplus k$, тоді:

$$ELP^{F_k}(\alpha, \beta) = [\alpha_x \oplus \beta_x \oplus L^*(\beta_y)] \left(\sum_u (-1)^{\alpha_y \cdot u \oplus \beta_y \cdot S(u)} \right)^2 =$$

$$= [\alpha_x = \beta_x \oplus L^*(\beta_y)] LP^s(\alpha_y, \beta_y),$$

операція $\cdot$ означає скалярний добуток. □

Нехай $G_{k_1,k_2}(x, y) = F^{(1)}_{k_1}(F^{(2)}_{k_2}(x, y))$ – функція, яка описує два раунди досліджуваної схеми MISTY; усереднені лінійні потенціали для функції G обчислюється за такою формулою [10]:

$$ELP^G(\alpha, \beta) = \sum_\gamma ELP^{F^{(2)}}(\alpha, \gamma) \cdot ELP^{F^{(1)}}(\gamma, \beta).$$

Дане співвідношення безпосередньо випливає з формули 1.3.

Позначимо $H_{k_1,k_2,k_3}(x, y) = F^{(3)}_{k_3}(F^{(2)}_{k_2}(F^{(1)}_{k_1}(x, y)))$ як функцію, яка описує три раунди нашої схеми. У такому випадку усереднений лінійний потенціал для функції H обчислюється за такою формулою:

$$ELP^H(\alpha, \beta) = \sum_\gamma ELP^G(\alpha, \gamma) \cdot ELP^{F^{(3)}}(\gamma, \beta).$$

Аналогічним чином можна отримати формули для обчислення

усередненого лінійного потенціалу від будь-якої кількості раундів.

Наведемо основні кроки подальших експериментальних обчислень. Спочатку було проведено генерування всіх можливих функцій L, ранг яких становить 2, загальна кількість таких функцій становить 42. Також було згенеровано всі можливі S-блоки бітової довжини 3; загальна кількість таких блоків перестановок становить $(2^n)!$, де n - кількість бітів на вході S-блока. У нашому випадку, загальна їх кількість становить $(2^3)! = 40320$.

Наступним кроком було відкинуто найгірші з точки зору стійкості до лінійного криптоаналізу (ті, на які можна легко провести атаку) S-блоки, тобто ті, для яких $MLP^S = 1$. Кількість S-блоків, для яких $MLP^S = 1$ становить 29568. Отже, після фільтрації залишилось усього 10752 S-блоків, для яких $MLP^S \neq 1$. Слід зазначити, що серед S-блоків, які залишилися після фільтрування, нема таких, для яких виконується співвідношення $MDP^S = 1$, тобто також не залишилося найгірших с точки зору стійкості до диференціального криптоаналізу.

Далі для кожної із 42 можливих функцій L було підраховано максимальні усереднені лінійні потенціали функції, яка описує r раундів нашої схеми для кожного із 29568 S-блоків й було обрано мінімальне значення $MELP^F$. Тобто ми будемо мати верхню межу для $MELP^F$ — це і буде верхньою границею із усіх можливих випадків. Іншими словами, ми будемо оцінювати найкращій із усіх найгірших випадків з точки зору стійкості до лінійного криптоаналізу для кожної із згенерованих функцій L.

Отримані розподіли верхніх оцінок для кожної L наведено для 3-раундової схеми на рис. 2.11, для 5-раундової схеми на рис. 2.12, для 6-раундової схеми на рис. 2.13 та для 7-раундової схеми на рис. 2.14, відповідно. Горизонтальна вісь показує номер досліджуваної функції L , вертикальна – мінімальне значення $MELP^F$ при функції L серед усіх S-блоків.

Розглянемо гістограму для трираундової схеми. Серед усіх можливих функцій L виділяються функції під номером 11-18, 21-24 та 33-40, для яких

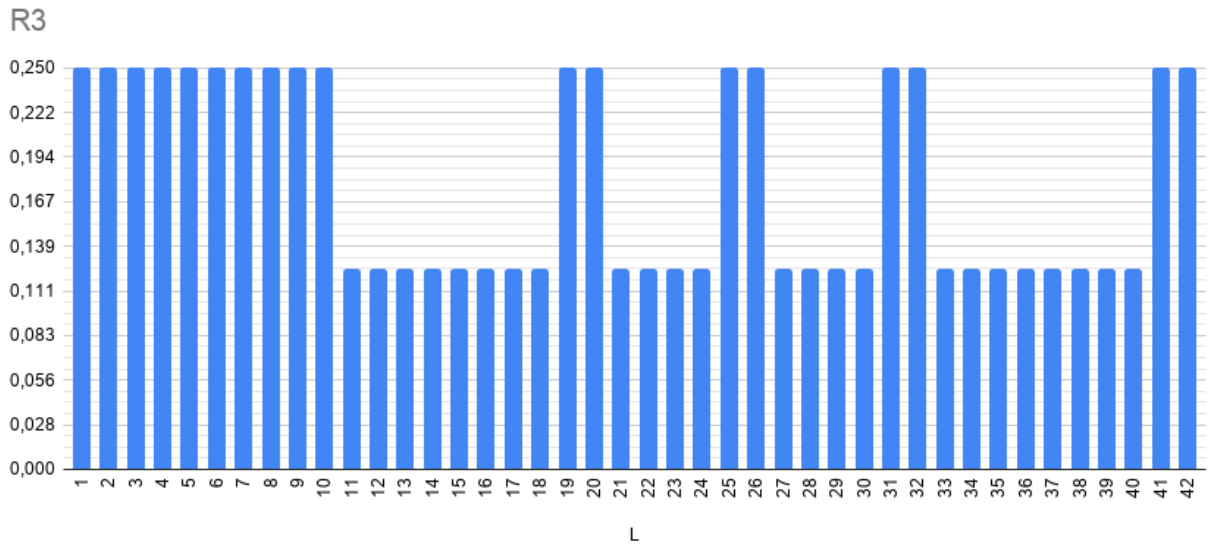

Рисунок 2.11 – Розподіл значень $MELP$ для схеми з трьома раундами для кожної L.

верхня межа $MELP = 0.125$, що вдвічі меньше за верхні оцінки для всіх інших функцій, для яких верхня межа $MDP = 0.25$.

Гістограми для чотирьох раундів приведено не було, оскільки при кожній функції L верхня оцінка становила $MELP = 0.09375$. Тобто ніяка серед усіх можливих лінійних функцій L не дає найкращих результатів.

Розглянемо гістограму для п'ятираундової схеми. Серед усіх можливих функцій L найменші показники $MELP$ досягаються для функцій під номером 11-14, 21-24, 27-30, 33-36, для яких верхня межа однакова і дорівнює $MELP = 0.041015$. На другому місці — функції 15-18 та 37-40, вони мають незначну перевагу над найкращими указаними вище функціями, однак вони є значно кращими за всі інші функції для яких показники стійкості суттєво не покращились по відношенню до найкращих починаючи від 3-го раунду.

Розглянемо гістограму для шестираундової схеми. Серед усіх можливих функцій L знову виділяються функції під номером 11-14 ,27-30 та 33-36, однак на відміну від попереднього раунду, функції 21-24 вже на другому місці, а не на першому. Також функції, які на п'ятому раунді за показниками були на другому місці, мають показники гірші за ті функції,

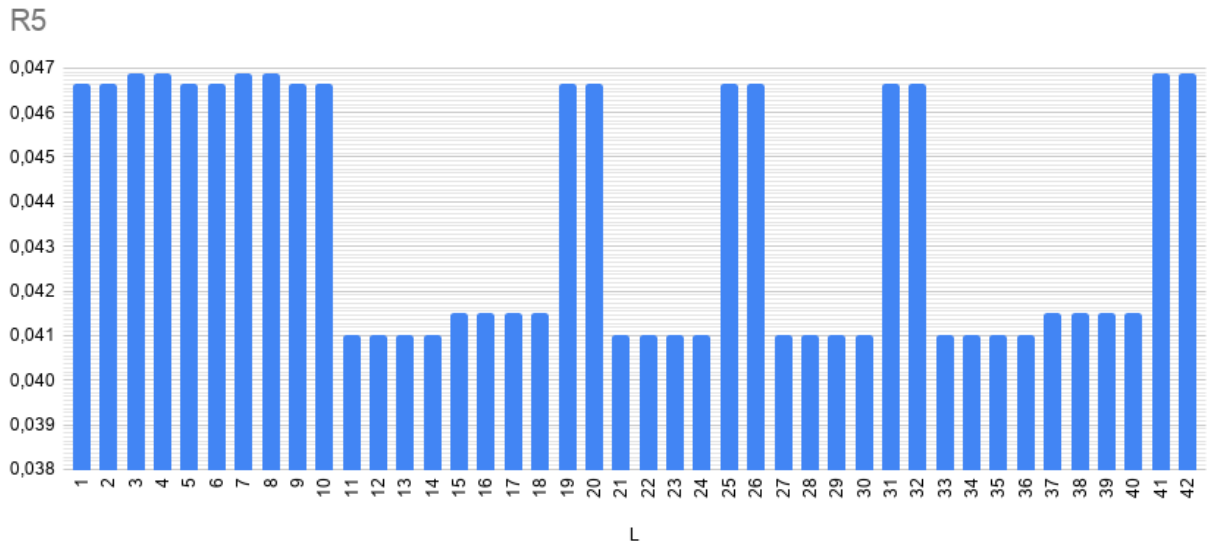

Рисунок 2.12 – Розподіл значень $MELP$ для схеми з пятьма раундами для кожної L

які протягом попередніх раундів мали найгірші показники $MELP$.

Розглянемо гістограму для семираундової схеми. На ній видно, що функції 21-24, які дали неочікувано гірший результат на попередньому раунді, несподівано показують гарний результат для семи раундів. Також слід виділити функції 15-18 та 37-40: вони за показниками стікості на другому місці, хоча для шестираундової схеми видно, що ці функції були на першому місці.

Із аналізу розподілів верхніх оцінок $MELP$ для всіх S- блоків при кожній із функції L було встановлено, що не вдається виділити такі L, які б давали найкращі нетривіальні верхні границі оцінки стійкості досліджуваної схеми на кожному із раундів шифрування, оскільки очевидно, що поведінка розподілів верхніх оцінок $MELP$ залежить від кількості раундів.

Функції L, які були найкращими з точки зору стійкості до диференціального криптоаналізу (у підрозділі 2.3 було встановлено, що це функції L за номером 5, 16, 17, 18 та 37, 38, 39, 40), у випадку для лінійного криптоаналізу поводять себе нестабільно, як було показано вище — вони не є найгіршими, однак їх не можна назвати найкращими.

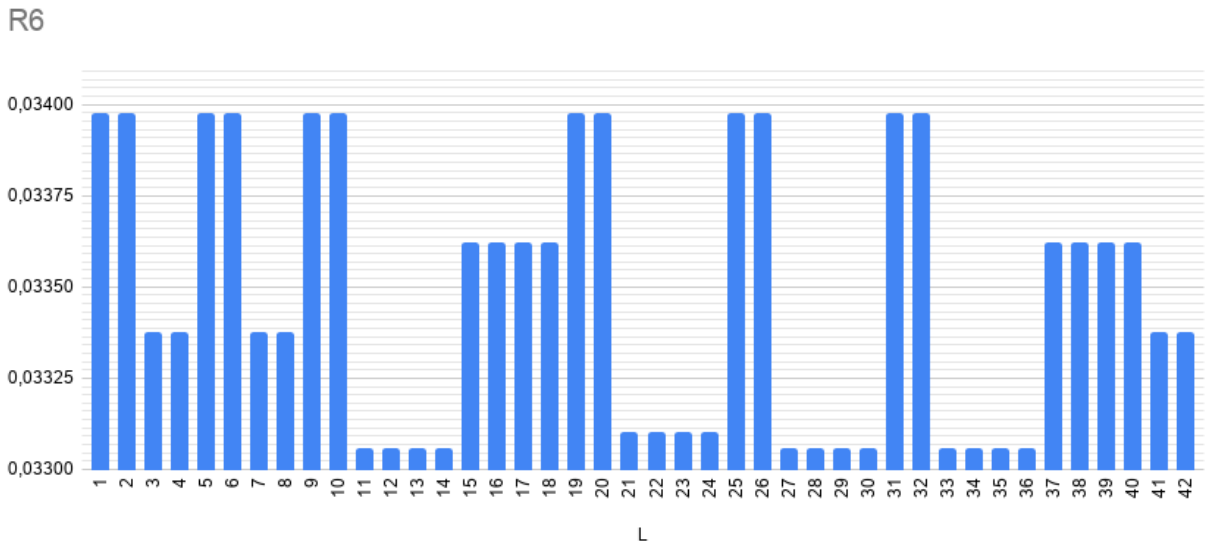

Рисунок 2.13 – Розподіл значень $MELP$ для схеми з шістьома раундами для кожної L

Висновки до розділу 2

Отже, була поставлена задача провести аналіз поведінки імовірності диференціалів та усереднених лінійних потенціалів для однорідної незбалансованої схеми $MISTY$, а також зрозуміти, наскільки лінійна частина (функція L) впливає на таку поведінку. Ця задача була експериментально вирішена.

Експериментальним шляхом було виявлено, що маніпулювання окремими складовими однорідної незбалансованої схеми MISTY такими як S-блок та лінійна функція може привести як до збільшення стійкості системи до диференціального криптоаналізу, так і до її зменшення. Одержані розрахункові результати показують, що для різних лінійних функцій L та для різної кількості раундів поведінка диференціальних імовірностей неоднозначна.

Взявши цей факт до уваги експериментально було отримано вісім найкращих функцій L з точки зору стікості до диференціального криптоаналізу в найгіршому з можливих випадків. Однак первинний

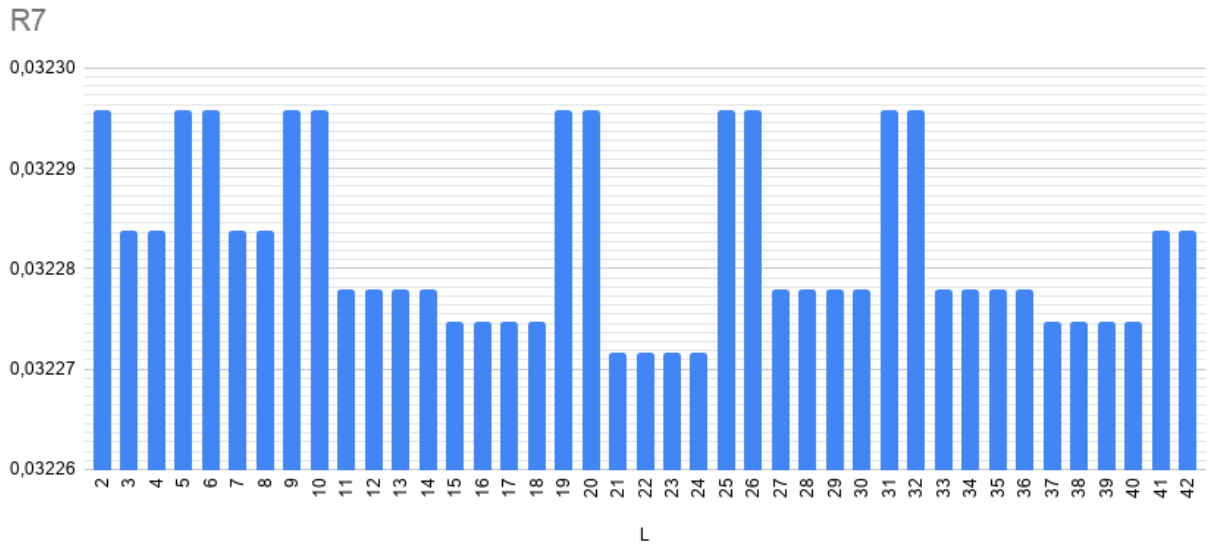

Рисунок 2.14 – Розподіл значень $MELP$ для схеми з сімома раундами для кожної L

аналіз отриманих найкращих лінійних перетворень показав, що для таких функцій не присутні явні особливості, що підсилюють стійкість досліджуваної схеми до диференціального криптоаналізу. Тому, скоріш за все, одержані результати не можна промасштабувати для таких схем зі збільшеним розміром.

Також есперементальним шляхом не вдалося отримати найкращих функцій L з точки зору стікості до лінійного криптоаналізу в найгіршому з можливих випадків, оскільки поведінка розподілів верхніх границь $MELP$ є нестабільною. Після цього ми дізналися, що функції L, які є найкращими з точки зору стійкості до диференціального криптоаналізу, не являються найкращими та найгіршими у випадку з лінійним криптоаналізом, оскільки їх поведінку не можна назвати стабільною.

ВИСНОВКИ

В ході даної роботи був проведений аналіз джерел та було показано, що до неоднорідних незбалансованих MISTY-подібних схем не приділялось достатньо уваги їх дослідженню, оскільки для таких схем не було опубліковано жодних оцінок стійкості до диференціального та лінійного криптоаналізу.

У роботі було проведено експериментальну оцінку стійкості модельного шифру малого розміру і статистично показано, як поводять себе максимуми ймовірностей диференціалів та лінійних потенціалів для такого шифру.

Було показано, що маніпулювання окремими складовими однорідної незбалансованої схеми MISTY такими як S-блок та лінійна функція може привести як до збільшення стійкості системи до диференціального криптоаналізу, так і до її зменшення. Одержані розрахункові результати показують, що для різних лінійних функцій L та для різної кількості раундів поведінка диференціальних імовірностей неоднозначна.

Експериментально було отримано вісім найкращих функцій L з точки зору стікості до диференціального криптоаналізу в найгіршому з можливих випадків, тобто такі функціїї дають гарантовану стійкість до атак збоку диференціального криптоаналізу, оскільки для будь-якого S-блока при таких функціях показник MDP шифру буде мати нетривіальну фіксовану верхню межу. Однак первинний аналіз отриманих найкращих лінійних перетворень показав, що для таких функцій не присутні явні особливості, що підсилюють стійкість досліджуваної схеми до диференціального криптоаналізу. Тому, скоріше за все, одержані результати не можна промасштабувати для таких схем зі збільшеним розміром.

Також есперементальним шляхом не вдалося виділити найкращі функцій L з точки зору стікості до лінійного криптоаналізу в найгіршому

з можливих випадків, оскільки поведінка розподілів верхніх границь $MELP$ є нестабільною. Згодом було показано, що функції L, які є найкращими з точки зору стійкості до диференціального криптоаналізу не являються найкращими та найгіршими по відношенню стійкості до лінійного криптоаналізу, оскільки, як було зазначено вище, їх поведінку не можна назвати стабільною.

У подальшому тематику даної роботи можна розвинути в напрямку побудови формальної теорії стійкості незбалансованих Фейстель-подібних схем до диференціального, лінійного та інших видів криптоаналізу.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Mitsuru Matsui. *New block encryption algorithm MISTY*. за ред. Eli Biham. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, с. 54—68. ISBN: 978-3-540-69243-0.

[2] Yuliang Zheng, Tsutomu Matsumoto та Hideki Imai. "On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses". в: *Advances in Cryptology — CRYPTO' 89 Proceedings*. за ред. Gilles Brassard. New York, NY: Springer New York, 1990, с. 461—480. ISBN: 978-0-387-34805-6.

[3] Bruce Schneier та John Kelsey. *Unbalanced Feistel networks and block cipher design*. за ред. Dieter Gollmann. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, с. 121—144. ISBN: 978-3-540-49652-6.

[4] Ковальчук Л.В. *Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа*. МГУ 25 – 27 октября 2006 г. – М.: МЦНМО, 2007. – С. 595 – 599.

[5] Kaisa Nyberg. ""Provable" Security against Differential and Linear Cryptanalysis". в: *Fast Software Encryption*. за ред. Anne Canteaut. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, с. 1—8. ISBN: 978-3-642-34047-5.

[6] Kazumaro Aoki. "On Maximum Non-averaged Differential Probability". в: *Selected Areas in Cryptography*. за ред. Stafford Tavares та Henk Meijer.

Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, с. 118—130. ISBN: 978-3-540-48892-7.

[7] Kaisa Nyberg. “Linear approximation of block ciphers”. в: *Advances in Cryptology — EUROCRYPT’94*. за ред. Alfredo De Santis. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, с. 439—444. ISBN: 978-3-540-44717-7.

[8] Mitsuru Matsui. *New structure of block ciphers with provable security against differential and linear cryptanalysis*. за ред. Dieter Gollmann. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, с. 205—218. ISBN: 978-3-540-49652-6.

[9] С. Яковлев. “Нестойкость несбалансированных схем Фейстеля к дифференциальному и линейному анализу”. рос. в: *Материалы XVI Международной научно-практической конференции «Безопасность информации в информационно-телекомуникационных системах»*. 2013, с. 62—63 с.

[10] Xuejia Lai, James L. Massey та Sean Murphy. *Markov Ciphers and Differential Cryptanalysis*. за ред. Donald W. Davies. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, с. 17—38. ISBN: 978-3-540-46416-7.